REMARKS

Reconsideration and allowance are respectfully requested.

The IDS filed on April 29, 2005 has not been formally acknowledged by the Examiner. Applicants respectfully request consideration and acknowledgement.

The specification is amended in light of U.S. patent practice. No new matter is believed added.

The reference numeral in claim 65 is removed. Withdrawal of the objection is requested.

Claims 52-54 stand rejected under 35 U.S.C. §112, second paragraph as allegedly being incomplete for omitting essential steps. This rejection is respectfully traversed.

Claim 52 finds example support in a non-limiting example embodiment like that shown in Figure 6. In this non-limiting example related to a configuration phase indicated above the dashed line, the stored secret C is used in conjunction with trigger data (config data) by the means for generating 15, to generating trigger data X. Claim 52 is not limited to this example in Figure 6. Withdrawal of the rejection is requested.

Claims 47, 48, 51-54, 58-64, 66, 67, 69-71, 73, and 75 stand rejected for obviousness under 35 U.S.C. §103 based on EP 1081891 to Hopkins in view of Challener U.S. 6,470,454. This rejection is respectfully traversed.

Paragraph [0032] of Hopkins teaches a security module 24 with a secure section 26 and an unsecured section 28. For the internally confined device specific security data, the Examiner points to paragraph [0039] in Hopkins and the private part/key KPVSS which remains within the target secure section 26 and is not communicated outside the target secure section 26. The Examiner admits that Hopkins does not explicitly disclose that the device-specific security data is generated by performing cryptographic processing on at least partially the stored secret.

The Examiner turns to the Challener reference for this missing claim feature and specifically points to the abstract as well as column 5, lines 28-50. At these lines, Challener is describing the flowchart in Figure 2. A serial number for a particular data processing is obtained from the user at block 403. The serial number is entered as an input to a cryptographic hash function. A secret key is entered at step 405 as another input to the hash function. At block 407, the cryptographic hash function computes a hash value which is processed to develop a password in block 409. The password is then distributed to the user at block 411.

But Challener's secret key is not tamper-resistantly stored and inaccessible over an external circuit interface, as recited in claims 47, 66, and 70. Indeed, Challener's secret key is not even stored on the device. In addition, neither Hopkins nor Challener teach cryptographic processing a tamper-resistantly stored secret and external data received external to the tamper-resistant electronic circuit to generate a temporal instance of device-specific security data internally confined with the electronic circuit during usage of the device as set forth in claims 47 and 70. Still further, neither reference teaches that "the generated temporal instance of device-specific security data depends on a value of said stored secret and a value of said external data" and that "the generated temporal instance of device-specific security data can only be generated as long as external data is available at the receiver" as recited in claims 47, 66, and 70.

In addition to the combination failing to teach multiple features recited in claims 47 and 70, the combination is legally improper because a person of ordinary skill in the art would not know how to combine the teachings of Hopkins and Challener. The secret key described by Challener et al. is not described as tamper-resistantly stored or inaccessible over an external circuit. As pointed out earlier, Challener's secret key is not even stored on the device. Assuming that the combination proposed by the Examiner envisions that the secret key in

Challener is stored on the device in Hopkins's secure section, the office action fails to explain what cryptographic processing of at least partially secret data generates internally-confined device-specific security data. Recall that Challener's secret key is used to generate a password. Because a password is entered by a user, it is not internally-confined. Applicants assume that the internally-confined device-specific security data of the proposed combination is represented by Hopkins's private key. But there is no teaching or suggestion of how Challener's password generated by cryptographic processing of the secret key and serial number is related to or used to derive Hopkins's private key.

Alternatively, the Examiner may be arguing that Hopkins's private key constitutes the tamper-resistantly stored secret, inaccessible over an external circuit and that the serial number in Challener and the private key in Hopkins are somehow cryptographically processed to generate the internally-confined device specific security data. But under this combination assumption, it is not clear what cryptographic operation is performed, what is the internally confined device specific security data, how to perform security-related operations, or what the security-related operations include. Challener teaches hash functions of two values to create a password that is distributed to the user, i.e., the password is not internally-confined. Hopkins teaches public key operations (encryption, digital signature) out of which only digital signatures is typically done with a private key. It is not clear how a digitally-signed serial number or similar would be internally-confined and used in a security-related operation.

Accordingly, because one of ordinary skill in art would not understand how to make the proposed combination, that combination is improper.

For multiple independent reasons explained above, the obviousness rejection should be withdrawn. The application is in condition for allowance. An early notice to that effect is requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: ______________________
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100